Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 333 – 341

Procedia Computer Science

Second International Symposium on Computer Vision and the Internet (VisionNet'15)

On Reduced Computational Cost, Efficient and Secure Routing (ESR) for Wireless Mesh Network

[a]Geetanjali Rathee, [b]Hemraj Saini*

[a, b]*Department of Computer Science & Engineering*
Jaypee University of Information Technology, Waknaghat-173234 INDIA

Abstract

Different next generation wireless network technologies are developed to provide better services to the community. WMN is considered as a novel wireless network archetype as it does not rely on any of the fixed infrastructures. However, there exist some challenging issues in designing of the WMN such as vulnerability towards malicious attacks and communication cost. Several routing protocols i.e. ARAN, SAODV or TAODV have been proposed but lead to above mentioned drawbacks. In this paper, a novel approach for Secure Routing Protocol is proposed which overcomes drawbacks like- high communication cost, man-in-middle attack, wormhole attack and rushing attack. Furthermore, the approach is proved by showing the proper simulation results.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Keywords: Internet; Wireless Mesh Network; Routing Protocol; Efficient Secure Routing (ESR), Ad-hoc network; Security

1. Introduction

As Ad-hoc networks [1] have a variety of applications in individual life but always visage copious challenges as a consequence of node mobility and high faking prospect. To provide better services, several networks develop into the next cohort; wireless mesh network (WMNs) [2-3] has emerged recently as a key technology. The extension of multi-hop Ad-hoc network is WMN; it is a combination of Ad-hoc and Mesh networking. Ad-hoc network is one

* Corresponding author. Tel.:+91 8894969853; fax: +91 1792 245362.
E-mail address: hemraj1977@yahoo.co.in

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.028

where each device can unswervingly converse with any other device within its broadcasting ranges while in mesh networks; each device acts as a router and has the proficiency to retransmit the data to a target node. Ad-hoc network is considered as a subset of WMN. Based on the functionality nodes, WMN architecture (as shown in figure 1) is classified into three main groups; i) infrastructure/backbone WMN; ii) client WMN and iii) hybrid WMN. All the three architectures of WMN, consist of three types of nodes; WMN client, WMN router and WMN gateway. **WMN client** is the termination user device that accesses the system for using the email, VoIP, gaming and location detection applications. The end user devices can be laptops, PDA's, smart phones etc. The WMN clients have limited power and routing capability [4-5]. It may or may not be connected to the network as it is mobile in nature. **WMN routers** route the traffic of network. The WMN mesh routers are reliable and have minimum consumption of transmission power. To enable the scalability in multi-hop mesh environment, MAC in mesh routers chains multiple channel and multiple interfaces [6]. **WMN Gateways** having direct access to the internet are expensive in nature as they have multiple interfaces to connect to wired/wireless networks [7].Wireless Mesh Network augments the performance of network because of flexible network architecture, easy configuration, deployment, resiliency and mesh connectivity. The cost of networking is continuing to decline and has become an essential part in completing daily business tasks. Advancement in network technology has allowed the organisations to use network not only to share resources but also to store large pool of data for analysis. So, securing such data and resource of organisations on a network is a big concern. No computer network is completely secure [21-22]. Wireless mesh networks guarantee to broaden the high-speed wireless connectivity ahead of what is possible with the current 802.11(WiFi-based infrastructure). However, their exclusive architectural traits leave them principally vulnerable to security threats.

Fig. 1. Wireless Mesh Network Architecture [2]

Security is generally defined as the state of being free from any danger or threat. The basic understanding about the security techniques is very important for the research being performed today. A network is a subject to attack from malicious sources. Because of the multi-hop communication environment and wireless media, ensuring security of an underlying routing protocol in wireless mesh network (WMN) is a crucial issue. Various attacks [8-10] on routing protocols can be defined as: worm hole attack, black hole attack, gray hole attack and sybill attacks. All these attacks can be dynamic or inactive in nature. Let us have a brief introduction of all these attacks. In Worm hole attack [11] two or more malicious devices conspire to form a channel, using an efficient communication system. Black hole attack [12], Even though a malicious node M does not have an effective route to endpoint, M always do a positive reply of RREQ messages and drops all the packets reaching toward the destination node. Black hole attack is easier to detect as it drops all the packets coming from the source node. Gray hole [13] attack is similar to black hole attack. In this instead of dropping all the packets it may discard some of the packets and finally Sybill attack [14] does type of attack where M creates multiple individualities in the network and each identity seem as a genuine node to access the network resources. To overcome these attacks, several routing protocols ARAN [15], SAODV [16], TAODV [17] have been proposed by several researchers in order to address the security vulnerability. In this work, we point out the liabilities of the vital existing secure routing protocols proposed for WMN. Also, we present a secure routing protocol tailored to WMN.

The paper is systematized in five sections. Section two demonstrates the execution of recently proposed approaches: ARAN [15] and SAODV [16] and TAODV [17] in WMN. Section three discusses proposed technique i.e. an Efficient Secure Routing (ESR). In section four we analyze the performance of proposed approach and finally we conclude the paper in section five.

2. Related Works

This section discusses various existing security routing protocols. The routing protocols established for ad hoc networks can be pragmatic to Wireless Mesh Networks as WMN share the mutual features with ad-hoc networks. ARAN [15], SAODV [16] and TAODV [17] use AODV [18] routing protocol as it is a combination of Dynamic Source Routing (DSR) [19] and Destination Sequence Distance Vector (DSDV) [20]. From DSR, AODV uses the concept of route discovery, route maintenance and hop by hop routing and hello messages from DSDV. AODV is a Reactive Routing Protocol for route construction and maintenance, it uses three type of control messages i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) by maintaining the routing table at intermediate nodes(as shown in figure 2(a) and (b)). The below subsection discusses the existing protocol with their limitation and features.

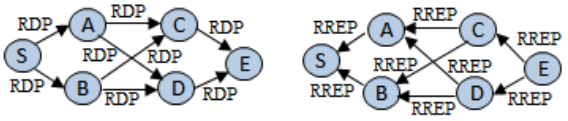

Fig. 2. (a) RREQ messages in AODV; (b) RREP messages in AODV

2.1. ARAN Routing Protocol

To provide the authentication against adversaries, ARAN customizes cryptographic certificates to meet the security goals. The route detection process in ARAN is proficient by broadcasting a route discovery message (RDM) while route reply messages are propagated in unicast fashion. During routing, all the nodes have the knowledge of certificate assigned by labeled CA (Certificate Authority). Whenever a new node (Mesh Router or Mesh Client) enters into a network, it must receive a certificate from CA (as shown in figure 3). The certificate assigned by CA includes Pu key of the node, issuance, and expiration time of the node, date of certificate and IP address of the new node. The certificate is coded by the Pr key of the source node. If a source node S wants to communicate with destination node D (as shown in figure 4). S develops route by sending package (RREQ message, certificate) to all its neighboring nodes. Package is explored and identified at each step. The following steps show the proper working of ARAN routing protocol.

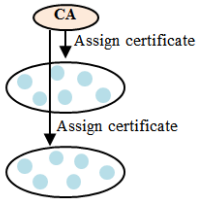

Fig. 3. ARAN Certificate AssignmentS

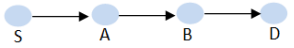

Fig. 4. RREQ Message

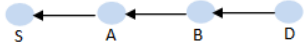

Fig. 5. RREP Message

Step 1: source node 'S' sends the package to intermediate node A
$((\text{RREQ}, \text{Dest.IP}, \#\ \text{Serial}, \text{Pu Source})\ \ \text{Prsource})$.
Step 2: Node A sends the corresponding package to node B after signing it.
$((\text{RREQ}, \text{Dest.IP}, \#\ \text{Serial}, \text{Pu Source})\ \ \text{Prsource})Pr_A$
Step 3: Node B verifies the signature by identifying the serial number and source pu key by detaching node's A signature and sends the corresponding package after signing it to node D.
$((\text{RREQ}, \text{Dest.IP}, \#\ \text{Serial}, \text{Pu Source})\ \ \text{Prsource})Pr_B$

Step 4: As package is reached to destination node D, node D follows the same procedure in reverse order. As shown in following steps using figure 5.

$((\text{RREQ, Dest. IP, \# Serial, Pu Source})Pr_{destination})$
$((\text{RREQ, Dest. IP, \# Serial, Pu Source})Pr_{destination})Pr_B$
$((\text{RREQ, Dest. IP, \# Serial, Pu Source})Pr_{destination})Pr_A$

The key features and drawbacks of ARAN are as follows.

2.1.1 Key features of ARAN

ARAN routing protocol is completely relying on certificate authority for the network security. The key features of ARAN protocol are discussed below:

- Every node which enters into the network has to get a Certificate signed by CA
- ARAN is based upon cryptographic certificates and relies on central trusted certification server.
- ARAN during route discovery sends RDP (Route Discovery Packet) to its neighbouring nodes.
- Upon receiving, intermediate nodes check the authenticity by verifying its certificate.
- Certificates are responsible for providing the authenticity of nodes.

2.1.2 Drawbacks of ARAN

Even though ARAN provides the security during communication but there exist several drawbacks as :

- It is based upon asymmetric coding and electronic signature which is vulnerable to dos attack
- Asymmetric coding is complicated task, costly and time consuming.
- It is completely dependent on CA and require signature verification at every step
- Highly vulnerable to worm hole attack (because of slow performance) and rushing attack(because of required time for decision making)

To remove such drawbacks, M.G. Zapata et. Al. have proposed another routing protocol i.e. SAODV (Secure AODV).

2.2. SAODV Routing Protocol

Another routing algorithm based on AODV is SAODV. To remove previous drawbacks and to improve the performance of networks, SAODV divides the routing package into two parts. i) Package changes the route; and ii) package which remains stable. Part one where package changes along the route uses hash codes while part second where package remains stable uses Pu keys. Stable Part of Package is defined as $(\text{RREQ, Dest IP, Pusource})Pr_{source}$ while unstable part of package is written as $(\#\text{serial})2 \text{ times hash code}$.

When source node S wants to convey some message to destination node D (as shown in figure 5), S first generate a random link and hashes it TTL(highest number of jumps allowed for a package) times. As in this case hashes 2 times as 2 intermediate nodes are there. Other hand, hash chains (developed using random links and hashing it in every step) is added to the header of package as $2(\#\text{serial})2 \text{ times hash code}$.

Now node receives the package, it explore whether two links added to the header are equal. If they are equal, receiver node confirms the accuracy of jump node, increases the jump by one and perform the hashing again. SAODV also uses electronic signature. Source node S signs the package before sending while intermediate nodes only validate it along the route. The same procedure applies in reverse direction.

2.2.1 Features of SAODV

SAODV routing protocol reduces the packet size by dividing the package into two parts. The features of SAODV protocol are:

- There is already a central key management system through which anyone can obtain its Pu key.
- Digital signatures are used to validate the field of messages.
- Hash chains are used to authenticate RREQ and RREP messages flowing between neighbouring nodes in the route detection process.

2.2.2 Drawbacks of SAODV

SAODV routing protocol is an enhancement over ARAN and able to remove the drawbacks of ARAN up to some extent but the major drawbacks in this are:

- Unsafe availability of node's Pr keys to other nodes.
- Possibility of MIM (Man in Middle) attack by invader node.
- Possibility of simulation adjacency feature by invader node.

To remove such drawbacks, authors have proposed another routing protocol i.e. TAODV.

2.3. TAODV Routing Protocol

The two routing protocols as discussed above includes certain type of drawbacks i.e. time consuming (as each node verifies the authenticity) and costly (digital signature signing, reduced performance). TAODV is a routing protocol where source node S needs to sign RREQ message and attach tickets. TAODV has three main entities: i) CA, ii) MR, iii) MC (as shown in figure 6).

2.3.1 TAODV set up

Initially all mesh routers (MR) and Mesh Clients (MC) will contact to CA to get the cryptographic details (as shown in step 1), then CA sends them cryptographic details (in step 2) from which MR and MC generate their own Pu or Pr keys (in step 3) and send their Pu keys to CA (in step 4).Whenever, new MR or MC join the network then following steps will be followed as shown below:

Step 1 each MR sends its certificate assigned by CA to AS
Step 2 AS after verifying the certificate issue ticket to MR
Step 3 CA send its certificate to MR for ticket request
Step 4 MR send its certificate and its ticket request to AS
Step 5 AS sends its tickets to MR
Step 6 MR Send the ticket to MC (As shown in figure 5)

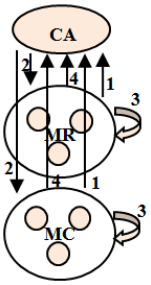

Fig. 6. TAODV Setup

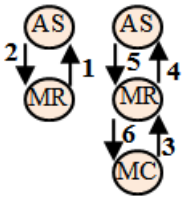

Fig. 7.New MR and MR join network

Let source S wants to communicate with destination node D. following steps will happen. S sends the message to A as $((RREQ, Dest.IP, timestamp)\ SKsource), T$. Then A sends the packet after verification to node B as $((RREQ, Dest.IP, timestamp)\ SKsource), T1, T2$ as shown in figure 7.

As packet reaches to node B, it verifies the ticket and forwards the packet by removing previous tickets and attaching its own ticket to destination node as $((RREQ, Dest.IP, timestamp)\ SKsource), T1, T3$. The same procedure will be followed in reverse direction.

2.3.2 Features of TAODV

TAODV routing protocol is an enhancement over ARAN and SAODV. The key features of TAODV are:

- Uses ticket based routing to provide security in network
- AS, CA, MR and MC are used to provide the security
- Encryption and decryption require less communication steps

2.3.3 Drawbacks of TAODV

As TAODV removes the previous protocol drawbacks but it still leads to several disadvantages:

- Both Authentication Server and Certificate Authorities are used
- Verification is done by opening the ticket and matching the source Pu key with the ticket(having S Pu key)
- Each time MC needs to contact to MR for ticket
- Uses asymmetric coding

So, to remove all these drawbacks, a new approach has been proposed which uses symmetric coding to provide the security in the network. Section III describes the new approach to provide security during routing.

3. Efficient Secure Routing (ESR) for WMN

In order to remove all such previous drawbacks, a novel technique is proposed to provide secure routing in the network. Instead of using asymmetric coding, symmetric coding technique is used. The proposed approach has 3 main entities (as shown in figure 8): **Pr key generator**- which is used to engender the private keys to mesh clients whenever mesh clients want to communicate with each other. **Authentication Server**- which is used to assign the tickets between mesh router and mesh client. And **Mesh clients**- which want to communicate with each other. To understand our algorithm efficiently, it is divided into three parts :i) path establishment ii) Security providence and iii) routing.

3.1. Path Establishment:

To improve the recital of the network, as a replacement of AODV routing protocol, any shortest path routing algorithm can be used. After path establishment, to provide the security inside the network, tickets and Pr key generators are used.

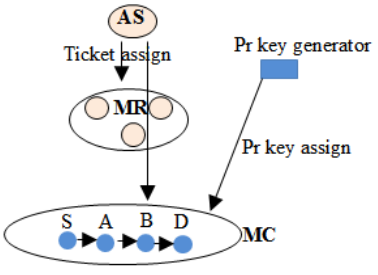

Fig. 8. ESR protocol

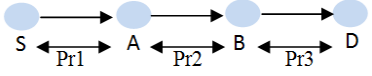

Fig. 9. ESR protocol

3.2. Ticket Assignment:

Whenever new Mesh Router (MR) or Mesh Client (MC) enters into the network, both MR and MC have to get their tickets from CA in order to provide the security during routing. Ticket of both MR and MC contain: $\text{Sid}, \text{Destid}, \text{exptime}, source_{Prkey}$.

3.3. Private(Pr) key Generator:

Pr key generator will be used only during transforming the packet from source S to destination D. Each paired node will generate their own Pr keys to minimize the routing threats. It is used to verify the authenticity of nodes during routing.

3.4. Routing Process:

Each node transmits the ticket and data, encryption by Pr keys of paired nodes. Data contains $Source_{Prkey}$, message and ticket contains S_{id}, $Dest_{id}$, Exp_{time}, $Source_{Prkey.}$ During verification if $Source_{Prkey}$ from data and $Source_{Prkey}$ of ticket match means it is valid and simply forwards the packet otherwise discard the node.

3.5. Working of ESR:

To understand the working of ESR let us consider figure 9. Every node has its tickets with it. After estaiblishing the shortest path from S to D (i.e. S-A-B-D) following steps will happen as shown below:

Step 1: S and A contact to Pr key generator for Pr1 to verify the authenticity of the nodes as $\text{Pr1}(\text{data}, \text{t1})$

Step 2: As packet reaches to node A, it will verify the ticket by matching the data $source_{Prkey}$ and Ticket $source_{Prkey}$

If (Data $source_{Prkey}$*==Ticket* $source_{Prkey}$*)*
{ Valid node/data
Forwards the packet to next node
}
Else
{ Invalid data
Discard the packet
}

Step 3: Node A removes ticket T1 after verification and send the data to node B using its own Pr key by attaching its own T2 as $\text{Pr2}(\text{data}, \text{t2})$.

Step 4: Similar process happens at node B i.e. removes the T2 after verification and forwards the data packet after encrypting with its own Pr key as $\text{Pr3}(\text{data}, \text{t3})$.

Finally data will reach to the destination node D securely.

3.6. Features and Advantages of ESR Algorithm

ESR protocol is able to remove all such previous drawbacks. The key features and pros of ESR are discussed below:

- Pr key generator is used only during routing process.
- Each neighbouring node has its own Pr key so that it is not easy to steal anyone's Pr key.
- Tickets are assigned initially to the network to reduce the overhead over CA
- Performance increases by using shortest path algorithm
- Instead of using the asymmetric coding, symmetric coding technique is used which is more efficient.
- To prove the above results, simulation of discussed routing protocols i.e. ARAN, SAODV, TAODV and ESR is done in ns2 and the results are shown in section IV.

4. Performance Evaluation

Computational Overhead is taken as an important parameter to prove the authenticity of the proposed approach. Computational overhead is defined as the minimum number of steps or computations (overhead) that a security protocol takes with routing algorithm. In case of asymmetric (Pu, Pr keys) coding, an extra overhead and memory is required to provide the security to the network. As ARAN, SAODV and TAODV use asymmetric coding and rely on a centralized server, so the number of communication steps increase between the client-server and server-server. While in case of ESR, a decentralized approach is used in which a Pr key generator is used during routing process only. Because of less number of computational steps and minimum interaction with Pr key generator, security is provided with minimum number of phases.

The simulation results of ARAN, SAODV, TAODV and ESR are shown below and it is proved that ESR is more efficient and secures routing protocol in comparison to all. ARAN, SAODV, TAODV use asymmetric coding technique so the corresponding computation cost of all these at each node is very high. TAODV is enhanced protocol over ARAN, SAODV. So as the number of nodes are increase, cost at each node increases simultaneously. The simulation is done over ns2. The default parameters of simulation are depicted in table 1. The corresponding table and graph are presented in table 2 and figure 10(a) and (b).

Table 1 simulation Parameters

Parameters	Size
No. of nodes	200
Area Size	500*500
MAC	802.11
Simulation Time	50 sec
Traffic source	CBR
Packet Size	512 bytes
Antenna	Omni Antenna

Table 2 Comparison of ARAN, SAODV, TAODV, and ESR

N(nodes)	ARAN	SAODV	TAODV	ESR
10	650	250	150	100
20	1430	350	266	215
30	2245	390	350	250
40	3489	500	355	300

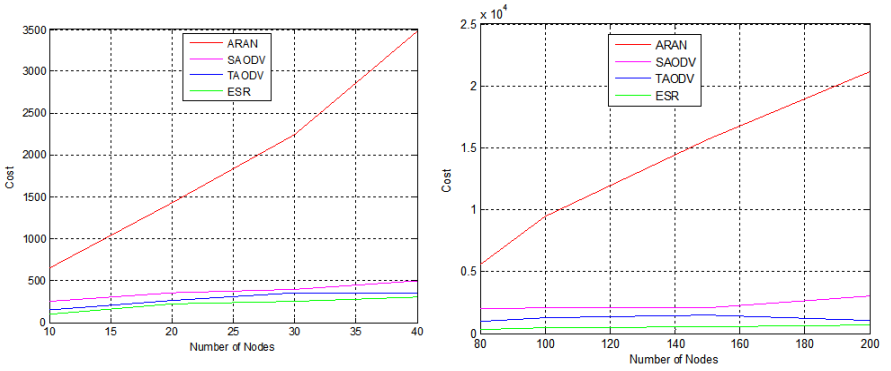

Fig. 10. (a) Comparing Computational cost of ARAN, SAODV and TAODV Routing Protocol; (b) Comparing computational cost of ARAN, SAODV, TAODV and ESR Routing Protocol

5. Conclusion

In this manuscript, an Efficient Secure Routing algorithm is proposed which ensures effective security in WMN with reduced computational cost. Symmetric key exchange techniques are used to provide security for this purpose. In the proposed approach, each node must communicate with the pr key generator during the routing of packets to enhance the security process. The comparison between previous proposed approaches (ARAN, SAODV, TAODV) and the proposed ESR approach is shown on different sizes and the enhancement is shown.

References

1. Gerla, Mario.Ad Hoc Networks. Ad Hoc Networks, Springer, US:2005.
2. Akyildiz, Ian F., and Xudong Wang.A survey on wireless mesh networks. In; IEEE conference on Communications Magazine, 43(9); 2005.
3. A. A. Franklin and C. S. R. Murthy. An introduction to wireless mesh networks. Security in Wireless Mesh Networks(book chapter), CRC Press,USA;2007.
4. J. Sen, N. Funabiki et al. Secure routing in wireless mesh networks. Wireless Mesh Networks (book chapter), INTECH, Croatia; 2011.
5. Y.-C. Hu, A, Perrig, and D. Johnson Ariadne: a secure on-demand routing protocol for ad hoc networks. Proceedings of ACM Annual International Conference on Mobile Computing (MobiCom'02), pp. 21 – 38, Atlanta, GA, USA; September 2002.
6. Y.-C. Hu, D.B. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, USA, pp. 3 – 13; June 2002.
7. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), , pp. 78 – 87, Paris, France; November 2002.
8. Padmavathi, Dr G., and Mrs Shanmugapriya. A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576 ;2009.
9. Mamatha, G. S., and Dr SC Sharma. Network Layer Attacks and Defense Mechanisms in MANETS-A Survey. International Journal of Computer Applications , pp-0975–8887;2010.
10. Siddiqui, Muhammad Shoaib, and Choong Seon Hong. Security issues in wireless mesh networks. International Conference on. IEEE Multimedia and Ubiquitous Engineering, MUE'07; 2007.
11. Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2), pp- 370-380 ; 2006.
12. Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. Black hole attack in mobile ad hoc networks. Proceedings of the 42nd annual Southeast regional conference. ACM; 2004
13. Sen, Jaydip, et al. A mechanism for detection of gray hole attack in mobile Ad Hoc networks. 6th International Conference on. IEEE Information, Communications & Signal Processing; 2007.
14. Douceur, John R. The sybil attack. Peer-to-peer Systems. In; Springer Berlin Heidelberg, pp-251-260 ;2002.
15. Sanzgiri, Kimaya, et al. Authenticated routing for ad hoc networks. IEEE Journal on Selected Areas in Communications, 23(3), pp- 598-610; 2005.
16. Zapata, Manel Guerrero. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review 6(3), pp- 106-107; 2002.
17. Qazi, S., Yi Mu, and W. Susilo. Securing wireless mesh networks with ticket-based authentication. 2nd International Conference on. IEEE Signal Processing and Communication Systems, ICSPCS ;2008.
18. Lee, Sung-Ju, and Mario Gerla. AODV-BR. Backup routing in ad hoc networks. IEEE conference on Wireless Communications and Networking Confernce, WCNC. , Vol. 3; 2000.
19. Johnson, David B., and David A. Maltz. Dynamic source routing in ad hoc wireless networks. Mobile computing. Springer pp- 153-181 US; 1996.
20. Perkins, Charles E., and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Computer Communication Review,24(4); 1994.
21. Saini, H. and Saini, D. VAIN. A Stochastic Model for Dynamics of Malicious Objects, ICFAI University journal of Systems Management, 6(1):14-28; 2008.
22. Saini, H. and Saini, D. Malicious Object dynamics in the presence of Anti Malicious Software, European Journal of Scientific Research, 18(3):491-499; 2007.